REMARKS

Reconsideration of the application in light of the following remarks is respectfully requested.

Status of the Claims

Claims 1-20 are pending in the application.

Rejections under 35 U.S.C. § 103

Claims 1, 2 and 15-17 were rejected under 35 U.S.C § 103(a) as being unpatentable over U.S. Patent No. 5,444,780 of Hartman in view of in view of U.S. Patent No. 6,590,981 of Fruehauf et al. ("Fruehauf"). Claims 3, 9-11, 19 and 20 were rejected under 35 U.S.C § 103(a) as being unpatentable over Hartman in view of Fruehauf and in view of U.S. Patent No. 6,944,188 of Sinha et al. ("Sinha"). Claim 4 was rejected under 35 U.S.C § 103(a) as being unpatentable over Hartman in view of Fruehauf and in view of U.S. Patent No. 6,510,236 of Crane et al. ("Crane") and U.S. Published Application No. 2002/0019933 of Friedman et al. ("Friedman"). Claims 5-8 and 12-14 were rejected under 35 U.S.C § 103(a) as being unpatentable over Hartman in view of Fruehauf and in view of U.S. Patent No. 5,982,506 of Kara. Applicant respectfully traverses these rejections.

Hartman describes a client/server secure timekeeping computer system. Hartman describes a server that encrypts a current time value from a highly accurate time-of-day clock, which is then sent to the client over an open communications channel. The client uses its own copy of a private key to decrypt the time value. Hartman, Abstract.

Fruehauf, at column 2, lines 22-34, merely describes that a multitude of keys, stored and/or generated by the system, are in hardware provided to an authorized user community (i.e., sender and receiver). The stored and/or generated keys are time synchronized in the authorized user community hardware so that the same key is used to encrypt data at the sending end as is used to decrypt the data at the receiving end. Fruehauf, column 2, lines 22-34. Fruehauf describes that the specific key for any particular time period is determined at the initialization of the system by the seed for remap units 105 and 122, which orders the key selection process for all of the synchronized hardware in the authorized user community. Fruehauf, column 4, lines 22-26. Periodic key changes are performed by the data encryptor 107 and the data decryptors 112-114 by obtaining a new key from the key storage units 104 and 117, respectively. Fruehauf, column 5, lines 1-5; Fig. 1.

Claim 1 of the present application recites "synchronously generating, at the central system and the network user, the at least one key." Claim 9 of the present application recites "a respective clock system at the network user and at the central system, wherein each of the respective clock systems is assigned to each other and configured to operate synchronously so as to generate at least one changed key." It is respectfully submitted that neither Hartman or Fruehauf, singly or in combination, disclose or suggest that a central system and a network user, or clock system at a central system for a network user, synchronously generate a key, as recited in claims 1 and 9, respectively. As acknowledged by the Examiner, Hartman does not teach synchronously generating, at the central system and the network user, the at least one key. Detailed Action, page 3, second to last paragraph. Nor does Fruehauf teach or suggest

synchronously generating a key at the user and central system, as recited in claims 1 and 9. In contrast, Fruehauf merely describes determining a specific key for a particular time at system initialization (Fruehauf, column 4, lines 22-26), and storing the keys into respective key storage units 104 and 117, where the sending unit and the receiving unit are synchronized to obtain new keys from the key storage units at predetermined periodic "key time" time periods (Fruehauf, column 4, lines 23-26, and column 5, lines 1-5). The respective keys of Fruehauf are not synchronously generated at both ends, as required by claims 1 and 9. Accordingly, a combination of Hartman and Fruehauf, to the extent proper, could not render claim 1, or dependent claims 2 and 15-17, obvious.

Regarding Sinha, Crane, Friedman, and Kara, it is respectfully submitted that these references singly or in combination, fail to teach or suggest the above-recited features of claims 1 and 9 missing from Hartman and Fruehauf. It is respectfully submitted therefore that respective combinations of Hartman, Fruehauf, Sinha, Crane, Friedman, and Kara, to the extent proper, could not render dependent claims 3-8, 10-14, 19 and 20, obvious.

Reconsideration of the respective rejections of claims 1-20 under 35 U.S.C. § 103(a) based on respective combinations of Hartman, Fruehauf, Sinha, Crane, Friedman, and Kara is respectfully requested.

CONCLUSION

In view of the foregoing it is believed that claims 1-20 are in condition for allowance and it is respectfully requested that the application be reconsidered and that all pending claims be allowed and the case passed to issue.

If there are any other issues remaining which the Examiner believes could be resolved through a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at the telephone number indicated below.

The Commissioner is hereby authorized to charge any unpaid fees deemed required in connection with this submission, including any additional filing or application processing fees required under 37 C.F.R. §1.16 or 1.17, or to credit any overpayment, to Deposit Account No. 04-0100.

Dated: June 2, 2009

Respectfully submitted,

By _____

Erik R. Swanson
Registration No.: 40,833
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(212) 527-7700
(212) 527-7701 (Fax)
Attorney For Applicant(s)